***Submit the completed PIA to***
***Privacy's SharePoint Customer Center***

# Diplomatic Clearance Application (DCAS) v2.0 PIA

## 1. Contact Information

| |
|---|
| **A/GIS Deputy Assistant Secretary** |
| Bureau of Administration |
| Global Information Services |

## 2. System Information

(a) Name of system: Diplomatic Clearance Application System

(b) Bureau: PM

(c) System acronym: DCAS

(d) iMatrix Asset ID Number: 879

(e) Reason for performing PIA:

☐ New system

☒ Significant modification to an existing system

☐ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable): Implementing system on a new technology platform to remediate security vulnerabilities and streamlining system functions. Basic system functionality remains the same. No changes to the data use associated with the system.

## 3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?

☒Yes

☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?

Legacy system underwent A&A in 2015; upgraded system will undergo A&A prior to deployment in 2017.

(c) Describe the purpose of the system:

DCAS supports the Bureau of Political-Military Affairs (PM) mission requirements for operational issues, military exercises, humanitarian operations, and administrative functions related to the joint efforts of the U.S. Department of State (DOS) and the Department of Defense.

The DOS PM Bureau is responsible for issuing diplomatic overflight/landing and vessel clearances. These clearances apply to all foreign military and foreign government owned, and on a case by case basis, civil charter flights transiting or landing and foreign state ship visits in the United States or its territories, often carrying foreign dignitaries or other luminaries.

The purpose of DCAS is to provide a web-based application for foreign embassies to electronically submit applications for diplomatic over flight or maritime clearance. Foreign embassies will use DCAS to manage over flight/maritime requests specific to their country. Other U.S. Government agencies [e.g., FAA and US Customs and Border Protection (CBP)] will have read-only access to the system to keep informed of foreign government flights coming into and out of U.S. airspace and territorial waters. All information transmitted is SBU and secured over a TLS connection.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:
The system collects low-sensitivity PII such as names, business addresses, telephone numbers, and email addresses of primarily non-U.S. citizens. Occasional U.S. citizen information may be entered from operators (e.g., pilots, ship captains, etc.); however, this information is limited. No social security, financial, or health data is included in DCAS.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?
Department of State's role and responsibility as per the Department of Homeland Security's National Strategy for Aviation Security.

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?
☐Yes, provide:
- SORN Name and Number:
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):

☒No, explain how the information is retrieved without a personal identifier.
Information is retrieved by application number

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☐Yes ☒No

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒Yes ☐No
(If uncertain about this question, please contact the Department's Records Officer at records@state.gov .)

If yes provide:

- Schedule number (e.g., (XX-587-XX-XXX)): A-24-050-01b
- Length of time the information is retained in the system: When records have reached their retention period of three years, they are handled according to the current Records Management Plan for DCAS.
- Type of information retained in the system:
  Clearance application case files

**4. Characterization of the Information**

(a) What entities below are the original sources of the information in the system? Please check all that apply.

☒ Members of the Public

☒ U.S. Government employees/Contractor employees

☒ Other (people who are not U.S. Citizens or LPRs)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?

☐Yes ☒No

- If yes, under what authorization?
DCAS does not collect SSNs

(c) How is the information collected?
Users enter the information via an online form in the DCAS web application

(d) Where is the information housed?

☒ Department-owned equipment

☒ FEDRAMP-certified cloud

☐ Other Federal agency equipment or cloud

☐ Other

- If you did not select "Department-owned equipment," please specify.
MS Azure FEDRAMP-certified cloud is being used for COOP; data is stored there in case contingency operations are required

(e) What process is used to determine if the information is accurate?
Users enter their own profiles and can edit information for accuracy. Federal staff conducts a manual review.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?
All information and applicable records are short-term records that correlate to flights and marine transportation. Once the flight/voyage is over, the record is no longer current and is available solely for reference.

(g) Does the system use information from commercial sources? Is the information publicly available?
No PII is collected from public or commercial sources. All information is access controlled.

(h) Is notice provided to the individual prior to the collection of his or her information?
Users provide the information as part of filling out the application for diplomatic clearance

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☐Yes ☒No

- If yes, how do individuals grant consent?
- If no, why are individuals not allowed to provide consent?
All DCAS information is required to fulfill the mission requirements. No unnecessary information is collected. Access to the system is based on consenting to a legal statement prior to logging into the system.

(j) How did privacy concerns influence the determination of what information would be collected by the system?
Personal information is required for PM to complete its diplomatic clearance mission. PM is responsible for issuing diplomatic overflight/landing and vessel clearances and uses the information contained in DCAS to do so. Only the least amount of personal information needed to support mission business functions is collected

## 5. Use of information

(a) What is/are the intended use(s) for the information?
The information is collected to provide data and metrics for review by appropriate USG agencies in order to clear foreign officials attempting to enter the U.S. This information is used strictly within DCAS and is not released to any other system or party.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?
Yes

(c) Does the system analyze the information stored in it? ☐Yes ☒No

If yes:

(1) What types of methods are used to analyze the information?

(2) Does the analysis result in new information?

(3) Will the new information be placed in the individual's record? ☐Yes ☐No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it?
☐Yes ☐No

## 6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.
The information is shared with the Federal Aviation Administration (FAA) and Customs and Border Protection (CBP), and the Department of Defense (DoD).

(b) What information will be shared?
All pertinent information for individual flight or marine travel is shared

(c) What is the purpose for sharing the information?
The purpose of sharing the information is to ensure all U.S. agencies involved are made aware of and provided the opportunity to prepare for the impending visit of a foreign aircraft/vessel. This includes vetting of personnel and any other applicable measures taken for security purposes while providing the tools to do so.

(d) The information to be shared is transmitted or disclosed by what methods?
All U.S. agency users are standard DCAS users who access the application via the DOS public web site. There is no direct interconnection.

(e) What safeguards are in place for each internal or external sharing arrangement?
Bureau policy and technical access controls

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?
Information sharing is based on the least amount necessary and involves only non-sensitive PII.

## 7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?
Standard web application login. Individuals submit their information via the portal, so they can login to access or correct their information.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?
☒Yes ☐No

If yes, explain the procedures.

All users can update their specific information in the DCAS application account web page

If no, explain why not.

(c) By what means are individuals notified of the procedures to correct their information?
DCAS users can change their personal information at any time via the account page; there is no notification per se. A user guide is available for their reference.

## 8. Security Controls

(a) How is the information in the system secured?
The information is secured using industry standard technologies, such as TLS encryption for data-in-transit and TDE encryption for the database. Access to information is restricted to approved users who have authorization to use DCAS.

(b) Describe the procedures established to limit access to only those individuals who have an "official" need to access the information in their work capacity.
All information is segregated by user role and account. The application and database structure does not allow unauthorized access to information not associated with the assigned user role. Ensuring only those with a need-to-know see the information when individuals at external agencies access DCAS is the responsibility of those agencies.

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?
Multiple safeguards include firewall, operating system, and application audit logs. The system is hosted in the IRM DMZ, which is utilizing its FISMA moderate security controls.

(d) Explain the privacy training provided to authorized users of the system.
All DOS users receive DOS privacy training via PS-800 (Cybersecurity Awareness) and PA-459 (Protecting Personally Identifiable Information). Foreign/outside users do not receive formal training, but are advised by and consent to a User Agreement prior to login that advises them regarding their security responsibilities.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? ☒Yes ☐No
If yes, please explain.
DCAS is available only via encrypted website (HTTPS) and transmits data by way of TLS with AES-256 encryption.

(f) How were the security measures above influenced by the type of information collected?

All security controls were put in place in the IRM DMZ in accordance with NIST 800-53 guidance for FISMA moderate level systems

## 9. Data Access

(a) Who has access to data in the system?

Authorized users, administrators, and the system owner have access to DCAS based on their assigned roles.

(b) How is access to data in the system determined?

Access to the data is dependent upon a person's assigned role and associated permissions as follows:

- Submitters only access their individual country's information
- Readers only access what PM authorizes them to see and can only add information applicable to their office
- Super Readers can only view all information with no ability to update or manipulate anything
- Administrators have full access to all DCAS data.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

User access is restricted for each user based on their assigned role and user account information within the application. Therefore, they can only see the information that is permitted based on their role and user account. Some users, such as the system owner and his delegates are "super users" who can access all data, as required.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

For regular users, technical controls are in place to prevent unauthorized browsing. For super users, policy and need-to-know are in place to prevent unauthorized browsing.